REMARKS

Applicant thanks the Examiner for the careful review of this application. Claims 1, 18 and 26 were amended to clarify aspects of the claimed embodiments. New claims 32-39 were introduced for consideration. No new matter was added. Claims 3 and 15 were previously canceled without prejudice. Therefore, claims 1-2, 4-14 and 16-39 are currently pending in this application.

REJECTIONS UNDER 35 U.S.C. § 103(a)

Claims 1-8, 11, 14, 16-19 and 21-31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over NetFlow in view of Jalalian (U.S. Patent No. 5,548,722). Claims 9 and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over NetFlow in view of Jalalian and further in view of FlowAnalyzer. Applicant respectfully traverses for the following reasons.

NetFlow apparently discloses a suite of products for monitoring and managing network traffic.

Flow Analyzer apparently discloses a network analysis tool that can be used to display network traffic information.

Jalalian apparently discloses a personal computer or workstation on a network that includes a quick-choice cache into which are collected the names and aliases of networked devices or services that are expected to be most routinely used by a particular user. The cache is initialized to contain the names and aliases of devices within a network zone assigned to the workstation. This collection of names/aliases is expanded each time the user makes a connection to a device not previously listed. The cache drives a graphic user interface (GUI) that shows the user what service categories are available within the cache, and then when a service category is selected, what specific devices are included within the cache under that service category. The GUI permits quick logical connection to devices whose aliases are stored in the user's cache.

A connection map later graphically shows the user what connections he or she has made.

The examiner alleges that the NetFlow user interface allows for configuration of bandwidth control parameters. Actually, the NetFlow user interface appears to simply state that it allows for configuration of the parameters by which NetFlow records are collected. In other words, NetFlow is a pure reporting tool that allows for analysis of resource utilization, etc. The NetFlow user interface gives a network administrator the ability to configure NetFlow's FlowCollector runtime, which controls how the data records are collected - not how the data flows themselves are controlled. Restated, in NetFlow, the control parameter relates to how flow records are collected and NetFlow does not teach network resource utilization control parameters.

As a result, Applicant respectfully submits that the combination of the NetFlow reference and Jalalian fails to achieve the claimed embodiments as their combination, even if appropriate to do so, would result in a pull-down menu of control parameters related to collection of NetFlow records and not control parameters related to utilization of network resources.

In view of the foregoing, withdrawal of the rejections of the claims is respectfully requested.

Regarding new claims 35 and 36, these claims are reflective of original claims 3 and 15.

Regarding new claims 37-39, the claims are directed toward methods and apparatuses for facilitating the configuration of a) control parameters controlling utilization of a network resource and b) configuration of bandwidth management parameters controlling bandwidth utilization. Control parameters and bandwidth utilization controls are hierarchically inter-related such that changing the bandwidth

utilization control, or control parameter, of the displayed traffic class to a higher-ranked or a lower-ranked bandwidth utilization control/control parameter causes a corresponding increase or decrease of priority for the bandwidth utilization or utilization of a network resource. Support for this claim limitation can be found in Applicant's specification and is repeated here for the Examiner's convenience:

> **Bandwidth management device 30 also supports bandwidth control categories. In one embodiment, administrator interface module 150 allows for the selection of a traffic class and the association of a bandwidth control category to it. See Figure 5. Bandwidth management device 30, in one embodiment, supports the following bandwidth control categories for inbound and outbound data flows separately: 1) Mission Critical, 2) Average, 3) Low Priority, 4) AutoDiscovered-Default, and 5) Prohibited. In one form, each bandwidth control category maps to a partition and/or a policy, whose parameters are configured to achieve desired bandwidth management objectives. For example, traffic classes associated with the "mission critical" category receive top priority, while data flows associated with "average" traffic classes can be restricted in order to give precedence to "mission critical" data flows. In addition, bandwidth controls for "low priority" data flows are configured such that they do not disrupt operations associated with "average" or "mission critical" data flows. Data flows associated with the "autodiscovered-default" category are data flows associated with traffic classes automatically discovered by traffic discovery engine 130 and not explicitly assigned to another bandwidth control category. Lastly, bandwidth controls associated with "prohibited" data flows are configured to block such flows.**
>
> -Applicant's specification, page 12, lines 4-21

Additionally, new claims 32-34 specify for only the most significant traffic or utilization classes to be displayed on a user interface that are greater than a percent threshold of the bandwidth utilization. This particular aspect is also disclosed in Applicant's specification:

> **In another embodiment, the most significant traffic classes are those traffic classes having utilization statistic values exceeding a threshold value (e.g., consuming more than a threshold percentage of aggregate bandwidth over an analysis interval).**

-Applicant's specification, page 16, lines 14-17

Applicant respectfully submits that the NetFlow documents and Jalalian do not disclose the claimed embodiments of claims 32-34 and 37-39, alone or in combination. Applicant does admit that the "Computing Resources for Residents" document, published by the University of Illinois at Urbana-Champaign ("UIUC") and cited by the Examiner in the previous Office Action, does disclose various rate-limiting restriction classes as indicated from the following section:

Rules & definitions of Rate-Limiting

Rate limiting for an IP address (an unique number assigned to each computer) is determined by the total bytes of Internet traffic accumulated in the previous 24 hours.

Unrestricted Class (10Mb/s): By default, connections are in this class. The connection is not artificially throttled or limited.

Restricted Class A (1.5Mb/s): When the Internet traffic of an IP address reaches 80% of the limit (600MB), the IP address (computer) will be rate-limited (throttled) to approximately the speed of a T1 line (about 15% of the bandwidth in the unrestricted class).

Restricted Class B (128kb/s): When the Internet traffic of an IP address reaches 100% of the limit (750MB), the IP address (computer) will be rate-limited (throttled) to approximately the speed of a dual ISDN line (about 1.28% of the bandwidth in the unrestricted class).

Restricted Class C (32kb/s): When the Internet traffic of an IP address reaches 150% of the limit (1125MB), the IP address (computer) will be rate-limited (throttled) to approximately the speed of a 33.6 modem (about .32% of the bandwidth in the unrestricted class).

The total Internet traffic for each IP address is checked every hour to calculate the total Internet traffic for the previous 24 hour period. Check gush at: http://gush.cso.uiuc.edu/my-internet from the IP address (computer) you wish to check. The previous 24 hour count will then be used to determine the class (transfer rate) your IP address is limited to. All of your traffic (Internet or UIUCnet) is affected by the class your connection is placed in. An exception to this is traffic between another computer on your floor or in your residence hall.

-UIUC, Rate Limiting for URHnet section

However, Applicant further respectfully submits that UIUC teaches away from using rate limiting dynamically in conjunction with multiple traffic classes. In marked contrast, UIUC specifically targets one traffic class (individual users) and applies rate limiting in a static fashion. That is, once a particular user exceeds certain throughput thresholds for a given time period, then rate limiting is imposed with no consideration for the network as a whole. For example, suppose it is spring break and the college dormitories are practically empty. One particular student couldn't afford to go to Florida with his friends so he is stuck at school and he is passing the time web surfing and

downloading music. After a few hours he starts to find that his connection is crawling to a halt because of the rate limiting policy detailed in UIUC. While the rate-limiting policy may contribute to keeping the network running smoothly while school is in session and lots of users are accessing the network, it makes little sense to limit that one student when there is plenty of network bandwidth available due to the low number of users on the network during the break.

The claimed embodiments use control parameters/bandwidth utilization controls in a dynamic manner in that the claimed embodiments facilitate association of control parameters/bandwidth utilization controls to displayed utilization classes. By providing methods and apparatuses to view network utilization as a whole and apply hierarchically inter-related controls, the claimed embodiments do not suffer from the above-described inefficiencies of the UIUC rate-limiting policies.

Telephone: (415) 826-7966